

Bestandsinspectie testen met Eicar

Inhoud

[Inleiding](#)

[Overzicht](#)

[Inzicht in het detectieproces voor Eicar](#)

[Samenvattend...](#)

Inleiding

In dit document wordt beschreven hoe bestandsinspectie met Eicar kan worden getest.

Overzicht

Op dit moment, wanneer u test of de functie Bestandsinspectie is ingeschakeld door de eicar.org test download bestanden te gebruiken, ziet u ander gedrag wanneer "SSL decoding" ingeschakeld of uitgeschakeld. Umbrella File Inspection scant alleen AV-downloads op eicar.org als SSL-decoding is ingeschakeld.

Inzicht in het detectieproces voor Eicar

Als u het blokkeren van eicar.org wilt inschakelen, [schakelt u SSL-decoding in](#).



Opmerking: SSL-decodering is vereist, zelfs bij een bezoek aan de site via HTTP. Als SSL-decodering niet is ingeschakeld, omzeilt de proxy domeinen die verkeer via HTTPS bedienen.

-
- De Umbrella Intelligent Proxy maakt een beslissing of een domein naar de proxy op de DNS-laag wordt verzonden.
 - Het DNS-verzoek vindt plaats vóór de HTTP/HTTPS-verbinding, wat betekent dat wanneer een domein is onderworpen aan de proxy, zowel HTTP- als HTTPS-verkeer altijd wordt benaderd.
 - Wanneer HTTP/HTTPS-verkeer onze Intelligent Proxy bereikt, is de eerste stap om een omleiding te maken om de gebruiker te identificeren.

Deze omleiding is niet mogelijk zonder SSL-decodering, wat betekent dat we in sommige scenario's (zoals Roaming-gebruikers) gebruikers mogelijk niet correct kunnen identificeren.

Om te voorkomen dat deze gebruikers HTTPS-verzoeken breken, gebruikt Umbrella geen proxy-domeinen (zoals eicar.org) die zowel HTTP- als HTTPS-verkeer dienen, tenzij SSL-decodering is

ingeschakeld.

Samenvattend...

Om de beste beveiliging en effectiviteit van de functie te krijgen, raden we ten eerste aan om de [Cisco Root CA](#) te installeren en SSL-decodering in te schakelen. Hierdoor kunnen testbestanden van eicar.org worden geblokkeerd en neemt het aantal domeinen toe dat onderworpen is aan bestandsinspectie via onze Intelligente proxy.

Hier is een samenvatting van het verwachte gedrag:

- SSL-decodering UIT
 - Eicar.org sites zijn NIET geblokkeerd op <https://www.eicar.org/download/eicar.com>. Het domein is gewoon helemaal niet geproxydeerd omdat SSL-decodering is uitgeschakeld.
 - Onze eigen testsite hosting eicar zijn geblokkeerd: <http://proxy.opendnstest.com/download/eicar.com>
- SSL-decodering ingeschakeld
 - Eicar geblokkeerd door AV-scanning op zowel <http://www.eicar.org/download/eicar.com> als <https://www.eicar.org/download/eicar.com>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.